ĐẢM BẢO AN TOÀN THÔNG TIN TRONG HỆ SINH THÁI GIÁO DỤC SỐ: TIẾP CẬN TÍCH HỢP TỪ CÔNG NGHỆ, QUẢN TRỊ VÀ VĂN HÓA SỐ

Nguyễn Thị Thúy Linh
Khoa Công nghệ Thông tin và Ngoại ngữ, Trường Cao đẳng Lào Cai

Tóm tắt: *Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, giáo dục không còn giới hạn trong không gian lớp học truyền thống mà đã mở rộng thành một hệ sinh thái số đa chiều, liên thông và phụ thuộc sâu sắc vào công nghệ. Sự phát triển này mang lại nhiều cơ hội nâng cao chất lượng đào tạo, nhưng đồng thời cũng đặt ra những thách thức nghiêm trọng về an toàn thông tin. Bài viết tiếp cận vấn đề an toàn thông tin trong giáo dục số dưới góc nhìn hệ sinh thái, phân tích các dạng rủi ro mới, mối liên hệ giữa an toàn thông tin và chất lượng giáo dục, đồng thời đề xuất các giải pháp mang tính tích hợp giữa công nghệ, quản trị và văn hóa tổ chức. Trên cơ sở đó, bài viết nhấn mạnh rằng an toàn thông tin không chỉ là một yêu cầu kỹ thuật mà còn là nền tảng để xây dựng môi trường giáo dục bền vững, tin cậy và hiệu quả trong thời đại số*
.

Từ khóa: *an toàn thông tin, giáo dục số, hệ sinh thái số, bảo mật dữ liệu, an ninh mạng, chuyển đổi số.*

ENSURING INFORMATION SECURITY IN THE DIGITAL EDUCATION ECOSYSTEM: AN INTEGRATED APPROACH FROM TECHNOLOGY, GOVERNANCE, AND DIGITAL CULTURE

Abstract*: In the context of rapid digital transformation, education is no longer limited to the traditional classroom but has expanded into a multidimensional, interconnected digital ecosystem deeply dependent on technology. This development brings many opportunities to improve the quality of training, but at the same time poses serious challenges regarding information security. This article approaches the issue of information security in digital education from an ecosystem perspective, analyzing new risk types, the relationship between information security and educational quality, and proposing integrated solutions involving technology, governance, and organizational culture. Based on this, the article emphasizes that information security is not only a technical requirement but also a foundation for building a sustainable, reliable, and effective educational environment in the digital age.*

Keywords: *information security, digital education, digital ecosystem, data security, cybersecurity, digital transformation.*

Nhận bài: 06/03/2026 *Phản biện: 23/03/2026* *Duyệt đăng: 27/03/2026*

I. ĐẶT VẤN ĐỀ

Chuyển đổi số trong giáo dục đã và đang làm thay đổi căn bản phương thức dạy học, quản lý và đánh giá. Không gian giáo dục truyền thống được thay thế hoặc bổ sung bởi các nền tảng học trực tuyến, hệ thống quản lý học tập (LMS), điện toán đám mây và các ứng dụng số đa dạng. Trong môi trường này, dữ liệu trở thành tài nguyên cốt lõi, đóng vai trò trung tâm trong việc cá nhân hóa học tập, đánh giá năng lực và ra quyết định quản lý.

Tuy nhiên, sự gia tăng nhanh chóng của các hệ thống số và mức độ phụ thuộc vào công nghệ cũng kéo theo những rủi ro nghiêm trọng về an toàn thông tin. Các cơ sở giáo dục ngày càng trở thành mục tiêu của các cuộc tấn công mạng, từ đánh cắp dữ liệu cá nhân, phá hoại hệ thống đến thao túng thông tin. Đặc biệt, đặc thù của môi trường giáo dục với số lượng lớn người dùng, trình độ công nghệ không đồng đều và sự phân tán dữ liệu càng làm gia tăng nguy cơ mất an toàn thông tin.

Trong bối cảnh đó, việc nghiên cứu và đề xuất các giải pháp đảm bảo an toàn thông tin trong giáo dục số không chỉ mang ý nghĩa bảo vệ hệ thống mà còn góp phần nâng cao chất lượng đào tạo, củng cố niềm tin của người học và thúc đẩy đổi mới giáo dục một cách bền vững.

II. NỘI DUNG NGHIÊN CỨU

2.1. An toàn thông tin trong giáo dục số dưới góc nhìn hệ sinh thái

2.1.1. Giáo dục số như một hệ sinh thái mở và phân tán

Giáo dục số hiện nay không còn là một hệ thống khép kín trong phạm vi nhà trường, mà đã chuyển dịch sang mô hình hệ sinh thái mở, nơi nhiều thành phần cùng tồn tại và tương tác trong không gian số. Hệ sinh thái này bao gồm không chỉ các chủ thể truyền thống như người học, giảng viên và nhà quản lý, mà còn mở rộng sang các nền tảng công nghệ, nhà cung cấp dịch vụ bên thứ ba, cộng đồng học tập trực tuyến và hệ thống dữ liệu liên thông.

Đặc điểm nổi bật của hệ sinh thái giáo dục số là tính phân tán cao của dữ liệu và quyền truy cập. Dữ liệu học tập không còn nằm tập trung trong máy chủ nội bộ mà được lưu trữ trên nhiều nền tảng khác nhau như điện toán đám mây, hệ thống quản lý học tập (LMS), ứng dụng học trực tuyến, thậm chí cả trên thiết bị cá nhân của người học. Điều này tạo ra sự linh hoạt trong học tập, nhưng đồng thời cũng làm gia tăng bề mặt tấn công (attack surface) của hệ thống.

Ngoài ra, sự phát triển của các công nghệ như trí tuệ nhân tạo (AI), dữ liệu lớn (Big Data) và Internet vạn vật (IoT) trong giáo dục càng làm cho hệ sinh thái trở nên phức tạp hơn. Ví dụ, các thiết bị học tập thông minh, lớp học ảo hay hệ thống đánh giá tự động đều thu thập và xử lý lượng lớn dữ liệu người dùng, từ đó làm gia tăng nguy cơ bị khai thác nếu không có cơ chế bảo mật phù hợp.

Một điểm đáng chú ý khác là sự phụ thuộc ngày càng lớn vào các nền tảng bên ngoài (third-party platforms) như Google Classroom, Microsoft Teams, Zoom,… Điều này khiến các cơ sở giáo dục không hoàn toàn kiểm soát được hạ tầng dữ liệu, dẫn đến các rủi ro liên quan đến quyền riêng tư và bảo mật thông tin.

2.1.2. Sự thay đổi bản chất của rủi ro an toàn thông tin trong môi trường giáo dục số

Trong mô hình giáo dục truyền thống, rủi ro an toàn thông tin thường mang tính cục bộ và dễ kiểm soát hơn do hệ thống được vận hành trong môi trường nội bộ (on-premise). Tuy nhiên, trong giáo dục số, rủi ro đã chuyển sang trạng thái đa chiều, liên kết và khó dự đoán hơn.

Trước hết, rủi ro không còn chỉ đến từ các cuộc tấn công bên ngoài mà còn xuất phát từ chính các hoạt động nội tại của hệ thống. Người dùng – bao gồm cả giảng viên và sinh viên – trở thành một phần của chuỗi rủi ro, khi hành vi sử dụng công nghệ thiếu an toàn có thể vô tình tạo ra các lỗ hổng bảo mật. Ví dụ, việc sử dụng cùng một mật khẩu cho nhiều tài khoản, đăng nhập trên thiết bị công cộng hoặc chia sẻ tài khoản học tập đều có thể dẫn đến mất kiểm soát thông tin.

Thứ hai, sự liên thông dữ liệu giữa các hệ thống làm gia tăng nguy cơ lan truyền rủi ro. Một lỗ hổng nhỏ trong một hệ thống có thể trở thành điểm khởi đầu cho một cuộc tấn công lớn, ảnh hưởng đến toàn bộ hệ sinh thái. Điều này đặc biệt nguy hiểm trong bối cảnh các hệ thống giáo dục ngày càng tích hợp sâu với nhau.

Thứ ba, dữ liệu trong giáo dục không chỉ là dữ liệu hành chính mà còn bao gồm dữ liệu hành vi, dữ liệu học tập, dữ liệu đánh giá năng lực – những loại dữ liệu có giá trị cao và nhạy cảm. Nếu bị khai thác, các dữ liệu này có thể bị sử dụng cho mục đích thương mại, thao túng hành vi hoặc xâm phạm quyền riêng tư của người học.

2.2. Tính liên kết giữa an toàn thông tin và chất lượng giáo dục

Trong bối cảnh giáo dục số, an toàn thông tin không chỉ là một yêu cầu kỹ thuật nhằm bảo vệ hệ thống, mà còn là một yếu tố có ảnh hưởng trực tiếp đến chất lượng giáo dục. Mối quan hệ này mang tính hai chiều: một mặt, mức độ an toàn thông tin quyết định tính ổn định và độ tin cậy của môi trường học tập; mặt khác, chất lượng giáo dục cũng phụ thuộc vào khả năng khai thác và bảo vệ dữ liệu một cách hiệu quả.

Trước hết, an toàn thông tin là điều kiện tiên quyết để đảm bảo tính liên tục của hoạt động dạy và học. Trong môi trường số, các hoạt động giảng dạy, kiểm tra – đánh giá, quản lý học tập đều phụ thuộc vào hệ thống công nghệ. Nếu xảy ra sự cố an ninh mạng như tấn công từ chối dịch vụ (DDoS), nhiễm mã độc hoặc mất dữ liệu, toàn bộ quá trình dạy học có thể bị gián đoạn, gây ảnh hưởng trực tiếp đến tiến độ và chất lượng đào tạo. Điều này đặc biệt nghiêm trọng trong các kỳ thi trực tuyến hoặc các hệ thống đánh giá tự động.

Thứ hai, an toàn thông tin góp phần đảm bảo tính chính xác và toàn vẹn của dữ liệu giáo dục. Dữ liệu học tập như điểm số, kết quả đánh giá, hồ sơ học tập là cơ sở để đưa ra các quyết định quan trọng liên quan đến người học. Nếu dữ liệu này bị thay đổi hoặc bị xâm phạm, sẽ dẫn đến sai lệch trong đánh giá, ảnh hưởng đến tính công bằng và minh bạch của hệ thống giáo dục. Do đó, việc đảm bảo tính toàn vẹn của dữ liệu là yếu tố cốt lõi để duy trì chất lượng đào tạo.

Thứ ba, an toàn thông tin có tác động lớn đến niềm tin của người học và các bên liên quan. Trong môi trường giáo dục số, người học thường phải cung cấp nhiều thông tin cá nhân và dữ liệu học tập. Nếu hệ thống không đảm bảo bảo mật, nguy cơ rò rỉ thông tin sẽ làm giảm niềm tin của người học, từ đó ảnh hưởng đến mức độ tham gia và tương tác trong quá trình học tập. Ngược lại, một môi trường học tập an toàn sẽ tạo điều kiện để người học chủ động chia sẻ, hợp tác và phát triển năng lực.

Bên cạnh đó, an toàn thông tin còn liên quan mật thiết đến khả năng đổi mới phương pháp giảng dạy. Các công nghệ như trí tuệ nhân tạo, dữ liệu lớn hay học tập thích ứng đều dựa trên việc thu thập và phân tích dữ liệu người học. Nếu không có cơ chế bảo mật phù hợp, các cơ sở giáo dục sẽ gặp khó khăn trong việc triển khai các công nghệ này do lo ngại về rủi ro dữ liệu. Như vậy, an toàn thông tin vừa là điều kiện, vừa là động lực thúc đẩy đổi mới giáo dục.

Một khía cạnh quan trọng khác là mối liên hệ giữa an toàn thông tin và chất lượng quản trị giáo dục. Trong hệ thống giáo dục số, các quyết định quản lý ngày càng dựa trên dữ liệu (data-driven decision making). Nếu dữ liệu không được bảo vệ và kiểm soát chặt chẽ, các quyết định đưa ra có thể thiếu chính xác, ảnh hưởng đến hiệu quả quản lý và chiến lược phát triển của nhà trường.

Từ những phân tích trên có thể thấy rằng, an toàn thông tin không chỉ đóng vai trò "bảo vệ" mà còn là một yếu tố "kiến tạo" chất lượng giáo dục. Việc đầu tư vào an toàn thông tin cần được xem như một phần không thể tách rời trong chiến lược nâng cao chất lượng giáo dục, thay vì chỉ là chi phí kỹ thuật. Trong bối cảnh chuyển đổi số, các cơ sở giáo dục cần nhận thức rõ mối liên hệ này để xây dựng các giải pháp đồng bộ, đảm bảo vừa phát triển công nghệ vừa duy trì chất lượng đào tạo một cách bền vững.

2.3. Giải pháp đảm bảo an toàn thông tin trong giáo dục số

Trong bối cảnh giáo dục số phát triển mạnh mẽ, việc đảm bảo an toàn thông tin cần được tiếp cận theo hướng tổng thể, tích hợp nhiều giải pháp từ công nghệ, quản trị đến con người. Không thể chỉ dựa vào một yếu tố đơn lẻ, mà cần xây dựng một hệ thống phòng vệ đa lớp, linh hoạt và thích ứng với các rủi ro ngày càng phức tạp.

Trước hết, về phương diện công nghệ, các cơ sở giáo dục cần đầu tư và triển khai các giải pháp bảo mật hiện đại nhằm bảo vệ hệ thống và dữ liệu. Việc mã hóa dữ liệu là yêu cầu cơ bản để đảm bảo thông tin được bảo vệ trong suốt quá trình lưu trữ và truyền tải. Bên cạnh đó, cần áp dụng các cơ chế xác thực mạnh như xác thực đa yếu tố (MFA) để hạn chế nguy cơ bị xâm nhập trái phép. Hệ thống tường lửa, phần mềm chống mã độc, cũng như các công cụ phát hiện và ngăn chặn xâm nhập (IDS/IPS) cần được triển khai đồng bộ nhằm giám sát và xử lý kịp thời các mối đe dọa. Ngoài ra, việc sao lưu dữ liệu định kỳ và xây dựng kế hoạch khôi phục sau sự cố (disaster recovery) là yếu tố quan trọng giúp đảm bảo tính liên tục của hoạt động giáo dục.

Thứ hai, về phương diện quản lý, cần xây dựng và hoàn thiện các chính sách an toàn thông tin phù hợp với đặc thù của từng cơ sở giáo dục. Các chính sách này phải quy định rõ ràng về quyền truy cập, trách nhiệm của từng cá nhân, cũng như quy trình xử lý khi xảy ra sự cố. Việc phân quyền truy cập cần được thực hiện theo nguyên tắc "quyền tối thiểu" (least privilege), đảm bảo mỗi người dùng chỉ được truy cập vào những dữ liệu cần thiết cho công việc của mình. Đồng thời, các cơ sở giáo dục cần thường xuyên thực hiện đánh giá rủi ro, kiểm tra an ninh hệ thống và cập nhật các bản vá bảo mật để kịp thời khắc phục các lỗ hổng. Việc tuân thủ các tiêu chuẩn và quy định về an toàn thông tin cũng là yếu tố quan trọng nhằm nâng cao tính chuyên nghiệp và đồng bộ trong quản lý.

Thứ ba, yếu tố con người đóng vai trò then chốt trong việc đảm bảo an toàn thông tin. Thực tế cho thấy, phần lớn các sự cố an ninh mạng đều có liên quan đến hành vi của người dùng. Do đó, việc nâng cao nhận thức và kỹ năng an toàn thông tin cho giảng viên, sinh viên và cán bộ quản lý là hết sức cần thiết. Các chương trình đào tạo, tập huấn cần được tổ chức thường xuyên nhằm trang bị kiến thức về nhận diện các mối đe dọa như lừa đảo trực tuyến (phishing), phần mềm độc hại, cũng như hướng dẫn cách sử dụng công nghệ một cách an toàn. Bên cạnh đó, cần xây dựng thói quen số an toàn như sử dụng mật khẩu mạnh, không chia sẻ thông tin cá nhân, và cảnh giác khi truy cập vào các liên kết không rõ nguồn gốc.

Ngoài ra, việc tăng cường hợp tác giữa các cơ sở giáo dục với các tổ chức chuyên môn về an toàn thông tin cũng là một giải pháp quan trọng. Thông qua hợp tác, các cơ sở giáo dục có thể tiếp cận với các công nghệ mới, chia sẻ kinh nghiệm và nâng cao năng lực ứng phó với các mối đe dọa. Đồng thời, cần thúc đẩy việc xây dựng các hệ thống giám sát an ninh mạng tập trung, cho phép phát hiện sớm và xử lý kịp thời các sự cố.

III. KẾT LUẬN

An toàn thông tin trong giáo dục số không chỉ là vấn đề kỹ thuật mà còn là yếu tố chiến lược ảnh hưởng trực tiếp đến chất lượng và sự phát triển bền vững của hệ thống giáo dục. Trong bối cảnh chuyển đổi số, các cơ sở giáo dục cần thay đổi cách tiếp cận, từ bảo mật đơn lẻ sang quản trị rủi ro toàn diện.

Việc kết hợp giữa công nghệ, quản lý và văn hóa sẽ tạo nên một hệ thống an toàn thông tin hiệu quả, góp phần xây dựng môi trường học tập tin cậy, thúc đẩy đổi mới giáo dục và nâng cao chất lượng đào tạo trong thời đại số.

TÀI LIỆU THAM KHẢO

Bộ Thông tin và Truyền thông. (2022). *Sổ tay hướng dẫn bảo đảm an toàn thông tin mạng trong cơ quan nhà nước.* Hà Nội.

Bộ Giáo dục và Đào tạo. (2021). *Chương trình chuyển đổi số trong giáo dục và đào tạo đến năm 2025, định hướng đến năm 2030.* Hà Nội.

International Telecommunication Union. (2020). *Global Cybersecurity Index 2020.* Geneva.

UNESCO. (2021). *Reimagining Our Futures Together: A New Social Contract for Education.* Paris.